The Application of Artificial Intelligence on Cybersecurity

A Technical Report submitted to the Department of Computer Science

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Jacqueline Lainhart
Fall, 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Briana Morrison
Department of Computer Science

The Application of Artificial Intelligence on Cybersecurity

CS4991 Capstone Report, 2023

Jacqueline Lainhart
Computer Science
The University of Virginia
School of Engineering and Applied Science
Charlottesville, Virginia USA
nyt8te@virginia.edu

ABSTRACT

Cybercriminals are constantly finding new and more secretive ways to steal information from people, which makes detecting these attackers increasingly difficult. Implementing the use of artificial intelligence (AI) can assist in real-time detection of threats. Model training utilizing user behavior, network logs, and previous attacks can produce algorithms that detect and protect users and networks. Specific algorithms can be created to address the different components that go into cybersecurity. The use of quantum computers alongside AI has the potential to break public key encrypted information. However, its harm might outweigh its benefit as it could negatively impact governments and economies through the data that can be stolen from them. Since quantum computing is looked at as the next step towards better AI algorithms, additional work is needed to implement regulations and quality assessments on AI models and quantum computing to ensure that people are protected against quantum encryption.

1. INTRODUCTION

With the growing landscape of technology and growing reliance on it, there are constantly new ways in which cybercriminals gather information. In this modern era, it is hard to find anyone who does not have any information stored digitally somewhere. Therefore, protecting data is a concern that many people share.

The─constant back and forth of detecting vulnerabilities and defending against them can make it difficult for humans to keep up with new threats, causing them to overlook flaws in systems. AI is a tool that can be used to combat threats, actively and proactively, faster than humans.

Even though the use of AI alongside cybersecurity has been explored for a number of years, AI is not developed with application to cybersecurity first in mind, and vice versa. Therefore, there is a desire to explore more applications of AI for cybersecurity. Some current approaches to cybersecurity have negative effects such as stifling functionality of web applications due to the preventatives put in place. Context reasoning is needed to assess the attacks occurring. AI can handle attacks in a way that attackers are not anticipating, which makes attacking harder for them.

However, AI is not the ultimate tool for cybersecurity because it presents its own flaws, especially if it is fed biased training data. Regulations can be put in place to help prevent these occurrences and ensure that an algorithm is properly maintained. Improving these algorithms to make them more effective requires a larger data set.

Quantum computing has the ability to handle larger data sets compared to classical computing. However, quantum computing has its own risks in that it can theoretically be powerful enough to break any encryption. Regulations and preventive measures against this emerging technology need to be considered.

2. RELATED WORKS

Morel (2011) highlights the importance of implementing AI in cybersecurity and the need to shift some of the focus of AI towards it. Experts might not be able to identify an attack occurring in real-time, though an AI algorithm might be able to. Morel explains that there could be a potential issue with false positives and false negatives occurring with these algorithms. My proposal would be to use large unbiased data and numerous comparison analysis that can be better handled with a quantum computer due to its multi-state nature. Even Morel mentions that solving issues with AI will be computably demanding.

Kashefi and Wallden (2019) note that seeking out quantum computing as a solution for better AI algorithms poses its own risk to cybersecurity, as the increased potential computational power has the ability to break into encrypted systems. They further explain how faster algorithms can be created with quantum computing than were possible with classical computing. They emphasize addressing preventative measures against post-quantum encryption now, as it is something that can take years to develop. Considering this only after quantum computing is implemented would be too late.

3. PROPOSED DESIGN

AI can consist of numerous kinds of machine learning algorithms. The best algorithm can change depending on the type of problem and data used (Alqahtani, et al., 2020). This is why numerous algorithms are tested to see if one yields better results than the other. Some of these paradigms include Bayesian, Decision Tree, Random Forest, Artificial Neural Network, and others. The kinds of datasets used for these algorithms for cybersecurity include ones from previous attacks and are categorized by the type of attack such as DoS attacks (Denial of service), remote to local attacks (R2L), user to root attacks (U2R), probe attacks, etc. The goal for these algorithms is to be able to identify an attack correctly and quickly.

The current use of AI in cybersecurity heavily relies on anomaly detection. Many services provided for cybersecurity are intrusion detection services (IDS). AI in cybersecurity focuses on anomaly-based attacks since those are the ones that can contain patterns for the algorithms to study and detect. “It examines the behavior of the network and finds patterns, automatically creates a data-driven model for profiling the expected behavior, and thus detects deviations in the case of any anomalies” (Alqahtani et al., 2020). The AI algorithms use data on previous attacks to make a prediction about whether or not an attack is present.

Existing AI tools from IBM such as QRadar can be used to monitor malicious activity and give suggestions on how to address potential threats. QRadar also features threat investigation where QRadar data mines and retrieves artifacts from a threat to assist the user in addressing it (IBM, 2023). AI2 is a platform developed by MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) in which it continuously takes input from human experts to improve its cyber-attack prediction. It has the capability of predicting 85% of attacks (Conner-Simons, 2016). Like QRadar, AI2 shows the information about a potential attack to a cyber-security analyst who confirms the attack. AI algorithms need human intervention to

confirm what is being assumed by the algorithms to prevent false positives or false negatives. Even though human intervention is required, AI algorithms are still useful because they are able to detect these anomalies more quickly than a human can and detect ones that a human might miss.

To take these algorithms for cybersecurity to the next level would be to implement machine learning algorithms using quantum computing. This would involve creating new algorithms that cannot be achieved through classical computing. One example is Shor's algorithm. Created in 1994, Shor's is a quantum algorithm designed to efficiently factorize large numbers, "The algorithm was viewed as important because the difficulty of factoring large numbers is relied upon for most cryptography systems" (Hayward, 2005). Personal data such as passwords are encrypted and stored through encryption, so attackers are not able to read what they are. Another aspect of cybersecurity besides attack detection and prevention is ethical hacking. Ethical hackers might need to decrypt this information, so using something like Shor's algorithm or AI intelligence created on a quantum computer could assist in breaking any kind of encryption.

4. ANTICIPATED RESULTS

With the implementation of quantum computing, the anticipated results include an "exponential sped-up over classical algorithms" (Shor, 1998). This is due to the way quantum computing is theorized to work. Bozzo-Rey, et al., (2019) explains that "a classical computer, for certain problems the solution is found by checking possibilities one at a time, which can take a long time. On a quantum computer, myriad possibilities emerge as probabilistic answers simultaneously."

With classical computing, a bit only takes in a 0 or 1. With quantum computing, quantum bits or qubit, as shown in Figure 1, can be both 0 and 1 simultaneously. This is called superposition. This is based on the electrical signals inside a computer where for quantum computing the electrical signal is from quantum particles, hence the name quantum computing (Brieler, et al., 2018). Because AI is created on a quantum computer, there is an expectation of exponentially faster anomaly detection. This kind of technology can assist in modeling molecules for drug creation, creating better machine learning algorithms that can be used for diagnosing patients or stock trading, handle big data analysis, assist in more accurate cyber defense (as mention), etc. (ID Quantique, 2023).

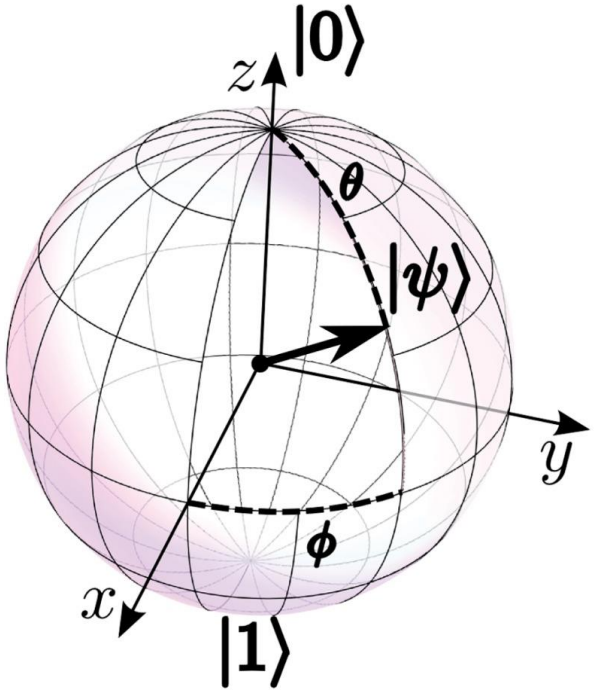

Figure 1: Diagram of a Qubit

5. CONCLUSION

With the ever-evolving landscape of cyber threats, it becomes more and more crucial to come up with new tactics to combat them. When trying to come up with new and innovative approaches for cybersecurity, many might forbode potential negatives that can

arise with these new technologies because they believe the societal benefits and monetary gain outweigh any harm. Using quantum computing to create better algorithms and such to hack into systems can have economical and health risks. There are already cases of people being able to hack into smart cars and control them. If quantum computing assists in these types of malicious attacks and increases the magnitude in which they occur, then death and a fear of technology is imminent. Therefore, it is important to consider the implications of a post-quantum world and have risk management in place whether it is through regulations or creating counter-algorithms.

6. FUTURE WORK

The first need is more research for AI in cybersecurity to make it more effective. This can involve the refinement of current algorithms, having a more ideal training set, exploring more approaches, etc. Researchers and industries can then come together to discuss any ethical concerns and further improvements to be made. To address the potential threats of quantum computing, there needs to be dedicated teams in the companies and countries that are investing in quantum computing that work to set up preventive measures against it.

Proposals are currently conceptual, since there are currently no quantum computers that are able to run algorithms that can potentially break encryptions. Even so, some conceptual proposals can expand upon the one that Mahadev proposes in which there can be protocols that the quantum computer must follow to prevent decryption of ciphertext or some policies that prevent data leakage (Kashefi & Wallden, 2019). These policies and proposals need to be standardized across nation-states and investors in quantum computing to decrease the risk of malicious intent and activity from occurring.

REFERENCES

Alqahtani, H., Sarker, I., Kalim, A., Hossain, S., Ikhlaq, S. & Hossain, S. (2020). Cyber Intrusion Detection Using Machine Learning Classification Techniques. 10.1007/978-981-15-6648-6_10.

Bozzo-Rey, M., Longbottom, J., & Müller H. A. (2019). Quantum computing: challenges and opportunities. *In Proceedings of the 29th Annual International Conference on Computer Science and Software Engineering (CASCON '19)*. IBM Corp., USA, 393–394. https://dl-acm-org.proxy1.library.virginia.edu/doi/10.5555/3370272.3370336

Brieler, J., Scherrer, J. F., & Solenov, D. (2018). The Potential of Quantum Computing and Machine Learning to Advance Clinical Research and Change the Practice of Medicine. *Missouri medicine*, *115*(5), 463–467.

Conner-Simons, A. (2016). *System predicts 85 percent of cyber-attacks using input from human experts.* Retrieved from MIT News: https://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

Hayward, M. (2005). Quantum Computing and Shor's Algorithm. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c4c3ad4aef68f3970d187fec0f13755471579018

ID Quantique. (2023). *Making Quantum Computing a Reality*. Retrieved from ID Quantique: https://www.idquantique.com/quantum-safe-security/quantum-computing/#:~:text=Quantum%20computers%20will%20allow%20much,to%20greater%20advancements%20in%20pharmacology.

IBM. (2023). *IBM Security QRadar Suite.* Retrieved from IBM: https://www.ibm.com/qradar

Kashefi, E., Wallden, P. (2019). Cyber Security in the Quantum Era. *Communications of the ACM*, *62*(4), 120. https://doi.org/10.1145/3241037

Morel, B. (2011). Artificial intelligence and the future of cybersecurity. *In Proceedings of the 4th ACM workshop on Security and artificial intelligence (AISec '11).* Association for Computing Machinery, New York, NY, USA, 93–98. https://dl.acm.org/doi/10.1145/2046684.2046699

Shor, P. W. (1998). Quantum computing. *Documenta Mathematica*, *1*(1000), 1.